PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants: Christian Hogl et al.	Examiner: Ojo O. Oyebisi
Serial No.: 10/018,237	Group Art Unit: 3692
Filed: June 24, 2002	Docket: 2043.184US1

Title: METHOD FOR TRANSMITTING A CODE

APPEAL BRIEF UNDER 37 CFR § 41.37

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

The Appeal Brief is presented in support of the Notice of Appeal to the Board of Patent Appeals and Interferences, filed on August 6, 2007, from the Final Rejection of claims 1-24 of the above-identified application, as set forth in the Final Office Action mailed on April 4, 2007.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of $510.00 which represents the requisite fee set forth in 37 C.F.R. § 41.20(b)(2). The Appellants respectfully request consideration and reversal of the Examiner's rejections of pending claims.

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, PAYPAL INC., as evidenced by the following:

An assignment from inventor Josef Gundel to Christian Hogl recorded July 30, 2002 at Reel 013141, Frame 0703; and

An assignment from Christian Hogl to PAYPAL, INC. recorded June 23, 2005 at Reel 016403, Frame 0720.

2. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants that will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

The present application was filed on June 24, 2002 with claims 1-11. Claims 12-22 were added in a Preliminary Amendment filed May 31, 2006. In response to the non-final Office Action mailed August 3, 2006, claims 23-24 were added. A Final Office Action (hereinafter "the Final Office Action") was mailed April 4, 2007. Claims 1-24 stand twice rejected, remain pending, and are the subject of the present Appeal.

4. STATUS OF AMENDMENTS

No amendments have been made subsequent to the Final Office Action mailed on April 4, 2007.

5. SUMMARY OF CLAIMED SUBJECT MATTER

This summary is presented in compliance with the requirements of Title 37 C.F.R. 5 41.37(c)(l)(v), mandating a "concise explanation of the subject matter defined in each of the independent claims involved in the appeal . . ." Nothing contained in this summary is intended to change the specific language of the claims described, nor is the language of this summary to be construed so as to limit the scope of the claims in any way.

Appellant's invention as claimed is directed at a mechanism for transmitting a code to a user (Specification: page 2 at 1st complete paragraph).

Claim 1 recites a method comprising receiving financial account identifier information of a user at a code allocation unit (Specification: at least page 1, page 2 at 3d complete paragraph); generating an access code for the user, the access code being to identify the user to a business entity (Specification: at least page 3 at 3d complete paragraph, page 5 at 2nd complete paragraph); and from the code allocation unit, effecting a value transfer utilizing the financial account identifier information and the access code, the access code being reflected in an amount of value associated with the value transfer so as to be transmitted to the user together with a receipt for the value transfer (Specification: at least page 2 at 3d complete paragraph).

Claim 12 recites a machine-readable medium having instruction data to cause a machine to: receive financial account identifier information of a user (Specification: at least page 1, page 2 at 3d complete paragraph); generate an access code for the user, the access code being to identify the user to a business entity (Specification: at least page 3 at 3d complete paragraph, page 5 at 2nd complete paragraph); and effect a value transfer utilizing the financial account identifier information and the access code, the access code being reflected in an amount of value associated with the value transfer so as to be transmitted to the user together with a receipt for the value transfer (Specification: at least page 2 at 3d complete paragraph).

Claim 23 recites a method comprising receiving financial account identifier information of a user at a code allocation unit (Specification: at least page 1, page 2 at 3d complete paragraph); from the code allocation unit effecting a money transfer transaction utilizing the financial account identifier information (Specification: at least page 5 at 1st complete paragraph); generating an access code for the user utilizing an amount of money associated with the money transfer transaction, the access code being to identify the user to a business entity (Specification: at least page 3 at 3d complete paragraph, page 5 at 2nd complete paragraph); and submitting the access code to be transmitted to the user together with a receipt for the money transfer transaction (Specification: at least page 2 at 3d complete paragraph).

Claim 24 recites a system comprising: a receiver to receive financial account identifier information of a user (Specification: at least page 1, page 2 at 3d complete paragraph); a generator generate an access code for the user, the access code being to identify the user to a business entity (Specification: at least page 3 at 3d complete paragraph, page 5 at 2nd complete paragraph); and a transfer module effect a value transfer utilizing the financial account identifier information and the access code, the access code being reflected in an amount of value associated with the value transfer so as to be transmitted to the user together with a receipt for the value transfer (Specification: at least page 2 at 3d complete paragraph).

This summary does not provide an exhaustive or exclusive view of the present subject matter, and Appellants refer to each of the appended claims and its legal equivalents for a complete statement of the invention.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Reilly (U.S. 5,877,482).

7. ARGUMENT

Claims 1-24 stand or fall together. Claim 1 is the representative claim. As discussed above, Appellants' invention as claimed is directed at a mechanism for transmitting a code to a user.

A) Applicable Law under 35 U.S.C. §103(a)

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka,* 490 F.2d 981, 180 USPQ 580 (CCPA 1974). An applicant is entitled to a patent unless "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1734, 82 USPQ2d 1385, 1391 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18, 148 USPQ 459, 467 (1966). See also KSR, 127 S.Ct. at 1734, 82 USPQ2d at 1391.

B) Overview of the System Disclosed in Reilly

Reilly is directed at a security system for EFT using magnetic strip cards. (Reilly, Title). In the background section, Reilly identifies the problem of card authentication being in that data encoded on a magnetic strip card can be readily generated from data transmitted to the computer system. Reilly explains that the problem irises because the card issuer has no proof that the transaction was originated on the basis of the physical card, because the transaction could have been generated from maliciously intercepted data contained in a previous transaction. (Reilly, 1: 49-55.)

Reilly proposes a solution where the part of the original card image that would have contained the card key is replaced by the product of a one way function containing at least one

specific detail of the transaction and the card key. Thus, states Reilly, cards that are manufactured from intercepted traffic can be readily identified as such. (Reilly, 3: 13-19.) This approach may include the use of a Personal Identification Number (PIN) provided to a customer. (Reilly, 3: 19-21.)

Reilly discloses performing PIN verification by either (i) decrypting the received PIN and comparing it to the stored PIN, or (ii) by encrypting the stored PIN and comparing it to the received encrypted PIN. (Reilly, 2: 46-64.) The PIN is encrypted using an encryption key. This *encryption key* is generated in Reilly for each transaction by using at least one specific detail of the transaction, such as the transaction amount. (Reilly, Abstract, 3: 9-13.)

C) Reilly fails to disclose or suggest each an every element of claim 1

The Office action states that "generating an access code for the user, the access code being to identify the user to a business entity" recited in claim 1 is disclosed in Reilly at Column 1, line 59 through Column 2, line 18. The associated text in Reilly is reproduced below.

> According to a first aspect, the present invention provides a method of encoding a magnetic strip card to enable validation of the card by an issuing organization during an electronic transaction, the method comprising the steps
>
> > (a) **generating a unique card key** for the magnetic strip card prior to issue, which is not readily derived from any other data recorded on the card,
> > (b) recording the card key on the magnetic strip of the respective card prior to issuing the card to a client,
> > (c) recording the card key with card details in a secure database.
>
> According to a second aspect, the present invention consists in a method of encoding a magnetic strip card to enable validation of the card by an issuing organization during an electronic transaction, the method comprising the steps of
>
> > (a) **generating a unique card key** for the magnetic strip card prior to issue, which is independent of any data visibly recorded on the card,
> > (b) **generating a Personal Identification Number (PIN)** associated with the card,
> > (c) recording the card key on the magnetic strip of the respective card prior to issuing the card and PIN to a client,
> > (d) recording the card key and PIN with card details in a secure database.

(Reilly, 1:59 - 2:18, emphasis added.)

As can be seen from the passage above, Reilly discloses "generating a unique card key" and also "generating a Personal Identification Number (PIN) associated with the card." The Office action does not specify whether it considers a unique card key or a Personal Identification Number (PIN) as corresponding to the "access code" recited in claim 1.

The "access code" recited in claim 1 is characterized by the feature of "being to identify the user to a business entity" and also by the feature of "being reflected in an amount of value associated with the value transfer." It is submitted that neither a unique card key nor a Personal Identification Number (PIN) disclosed in Reilly is "being reflected in an amount of value associated with the value transfer," recited in claim 1.

The Office action further cites Reilly at Column 3, lines 1-28 to show "the access code being reflected in an amount of value associated with the value transfer" recited in claim 1. The associated text in Reilly is reproduced below.

> Typically, the transaction details transmitted by the transaction terminal to the issuing body will include the transaction value, a transaction serial number and a code identifying the transaction terminal. In a financial transaction, the transaction value will be the financial value of the transaction, however, in other types of transactions, the value will have another relationship with the transaction data.
>
> In a preferred embodiment at least **one specific detail of each transaction is used as a second key** when encrypting the PIN. The specific detail being one of the details transmitted to the issuing body and the issuing body using the second key with the card key to de-crypt the PIN. Comparing the proposed transmission format with prior art formats, the part of the original card image that would have contained the card key is replaced by the product of a one way function containing at least one specific detail of the transaction and the card key. Thus, cards which are manufactured from intercepted traffic can be readily identified as can the source of the data used to manufacture them. This protection is afforded to card images and transactions with and without the use of a PIN.
>
> (Reilly, 1:59 - 2:18, emphasis added.)

As can be seen from the passage above, Reilly discloses "a second key" that is separate from the card key and is used together with the card key to de-crypt the PIN. It is also evident

from the above-reproduced that the "second key" is not used "identify the user to a business entity," as recited in claim 1, but is rather used to decrypt the PIN.

It is submitted that, while Reilly discloses *the use of the transaction amount in relation to an encryption key*, Reilly does not disclose or suggest an access code "being to identify the user to a business entity" and also "being reflected in an amount of value associated with the value transfer," as recited in claim 1.

Thus, the approach in Reilly utilizes a transaction amount with respect to an encryption key, but in no way with respect to a code that is used in Reilly to identify the user to a business entity (e.g., the PIN). Applicant would like to point out that this distinction between the system disclosed in Reilly and the features recited in claim 1 has already been outlined in response to the Office action mailed on August 3, 2006. The language from the previous response is reproduced below.

> In a preferred embodiment in Reilly, at least one specific detail of each transaction, preferably *the transaction value, is used as a second key when encrypting the PIN*. The specific detail is transmitted to the issuing body, and the issuing body uses the second key with the card key to decrypt the PIN. (Reilly, 3: 9-23.) Each one of the "encrypting" and "decrypting" is distinct from the "identifying." Specifically, a value used to encrypt the PIN or to decrypt the PIN is distinct from an access code to identify the user to a business entity. Thus, while Reilly discloses a transaction value being used as a second key when encrypting the PIN and that can be used by the card issuing body to decrypt the PIN, Reilly does not disclose or suggest **the access code "being to identify the user to a business entity" and "being reflected in an amount of value associated with the value transfer**," as recited in claim 1. No additional reference has been cited in the Office action to show this feature.
>
> (Response to the Office action mailed on August 3, 2006.)

In the Response to Arguments section, the Office action did not address the earlier assertion by Applicant that, in Reilly, a transaction value has no relationship to the PIN itself, but

is merely used to generate an encryption key, and that operations of "encrypting" and "decrypting" are distinct from the operation of "identifying." Instead, the Office action refers to the Abstract in Reilly that describes using an amount of the transaction to produce *a unique PIN key*. It is stressed yet again that a unique PIN *key* in Reilly is *an encryption key* used to encrypt the PIN (Reilly, 3: 9-19), where the key is distinct from the PIN itself. It is also submitted that Reilly does not suggest that a unique PIN *key* is suitable for any purpose other than encrypting/decrypting the PIN. There is no indication in Reilly that a unique PIN *key* can be used as **an access code "being to identify the user to a business entity" and "being reflected in an amount of value associated with the value transfer**," as recited in claim 1.

The Office action takes Official Notice that an electronic funds transfer terminal (EFT) is to produce a receipt of a transaction to a customer, including information from which to identify the specific transaction (a confirmation number). The Official notice does not remedy the deficiency of Reilly in failing to disclose "generating an access code for the user, the access code being to identify the user to a business entity" and "effecting a value transfer utilizing the financial account identifier information and the access code, the access code being reflected in an amount of value associated with the value transfer," as recited in claim 1.

Because Reilly, whether considered separately or in combination with the Official Notice of an EFT terminal to produce a receipt for the value transfer, fails to disclose each and every element of claim 1, claim 1 and its dependent claims are patentable in view of the combination of Reilly and the Official Notice and should be allowed.

SUMMARY

Appellants respectfully request the Board reverse the rejections of Claims 1-24 under 35 U.S.C. § 103(a) and direct the Examiner to enter a Notice of Allowance for Claims 1-24.

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. Box 2938
Minneapolis, MN 55402

Date October 18, 2007 By /Elena Dreszer/
Elena B. Dreszer
Reg. No. 55,128

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief- Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 29 day of October 2007.

Peter Rebuffoni
Name

Signature

8. CLAIMS APPENDIX

1. A method comprising:

receiving financial account identifier information of a user at a code allocation unit;

generating an access code for the user, the access code being to identify the user to a business entity; and

from the code allocation unit, effecting a value transfer utilizing the financial account identifier information and the access code, the access code being reflected in an amount of value associated with the value transfer so as to be transmitted to the user together with a receipt for the value transfer.

2. The method of claim 1, wherein the value transfer is a money withdrawal transaction.

3. The method of claim 1, wherein the generated access code is equal to the amount of money associated with the value transfer.

4. The method according to claim 1, wherein the value transfer is a money deposit transaction.

5. The method according to claim 1, wherein the effecting of the value transfer is by a remote data connection.

6. The method according to claim 1, wherein the access code is to be transmitted to the user by one or more of a remote data connection and an account balance statement printer.

7. The method according to claim 6, wherein the remote data connection is a computer network or an automated telephone interface.

8. The method according to claim 1, wherein:

the access code comprises at least two partial codes; and

a first partial code from the at least two partial codes is to be transmitted to the user together with the receipt for the value transfer and a second partial code from the at least two partial codes is to be transmitted by an alternative method to the user.

9. The method according to claim 1, further comprising receiving the identification data of the user at the code allocation unit.

10. The method according to claim 1, wherein the financial account identifier information comprises at least one of a group including:

data associated with a bank account number; and

data associated with a credit card number of the user.

11. The method according to claim 1, further comprising receiving the receipt for the value transfer at the allocation unit.

12. A machine-readable medium having instruction data to cause a machine to:

receive financial account identifier information of a user;

generate an access code for the user, the access code being to identify the user to a business entity; and

effect a value transfer utilizing the financial account identifier information and the access code, the access code being reflected in an amount of value associated with the value transfer so as to be transmitted to the user together with a receipt for the value transfer.

13. The machine-readable medium of claim 12, wherein the value transfer is a money withdrawal transaction.

14. The machine-readable medium of claim 12, wherein the access code is reflected in an amount of money associated with the value transfer.

15. The machine-readable medium according to claim 12, wherein the value transfer is a money deposit.

16. The machine-readable medium according to claim 12, wherein the code allocation unit is to effect the value transfer by a remote data connection.

17. The machine-readable medium according to claim 12, wherein the access code is to be transmitted to the user by one or more of a remote data connection and an account balance statement printer.

18. The machine-readable medium according to claim 17, wherein the remote data connection is a computer network or an automated telephone interface.

19. The machine-readable medium according to claim 12, wherein:

the access code comprises at least two partial codes; and

a first partial code from the at least two partial codes is to be transmitted to the user together with the receipt for the value transfer and a second partial code from the at least two partial codes is to be transmitted by an alternative method to the user.

20. The machine-readable medium according to claim 12, wherein the code allocation unit is to receive identification data of the user.

21. The machine-readable medium according to claim 12, wherein the financial account identifier information comprises at least one of a group including:

data associated with a bank account number; and

data associated with a credit card number of the user.

22. The machine-readable medium according to claim 12, wherein the code allocation unit is to receive the receipt for the value transfer.

23. A method comprising:

receiving financial account identifier information of a user at a code allocation unit;

from the code allocation unit effecting a money transfer transaction utilizing the financial account identifier information;

generating an access code for the user utilizing an amount of money associated with the money transfer transaction, the access code being to identify the user to a business entity; and

submitting the access code to be transmitted to the user together with a receipt for the money transfer transaction.

24. A system comprising:

a receiver to receive financial account identifier information of a user;

a generator generate an access code for the user, the access code being to identify the user to a business entity; and

a transfer module effect a value transfer utilizing the financial account identifier information and the access code, the access code being reflected in an amount of value associated with the value transfer so as to be transmitted to the user together with a receipt for the value transfer.

9. EVIDENCE APPENDIX

None.

10. RELATED PROCEEDINGS APPENDIX

None.